

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

## In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)SUBJECT PREMISES (2224 202nd St SW,  
Lynnwood, WA 98036), SUBJECT PERSON, and  
SUBJECT VEHICLE

Case No. MJ23-109

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SUBJECT PREMISES/PERSON?VEHICLE as further described in Attachment A

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

## Code Section

18 USC 2422(b), 2251(a), (e),  
and 2252(a)(2), (b)(1)

## Offense Description

Enticement of a Minor, Production of Child Pornography, and Receipt/Distribution of  
Child Pornography

The application is based on these facts:

- ☒ See Affidavit of, continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested  
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Alaina Dussler, Special Agent

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 03/07/2023

Judge's signature

City and state: Seattle, Washington

S. Kate Vaughan, United States Magistrate Judge

Printed name and title

I, Alaina Dussler, being duly sworn, depose and state as follows:

1. I am a Special Agent (“SA”) with the Department of Homeland Security (“DHS”), U.S. Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”). I have held such a position since December 2021. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. I am currently assigned to the Office of the Special Agent in Charge (“SAC”), Seattle, Washington, and am a member of the Child Exploitation Investigations Group. As part of my current duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have also had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)).

2. As part of my current duties as an HSI Criminal Investigator, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code, Sections 2251(a), 2252(a)(2), 2252(a)(4)(B), and 2243(a)(1). I have received training about child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography in various forms of media, including media stored on digital media storage devices such as computers, tablets, cellphones, etc. I am a graduate of the Criminal Investigator Training Program (“CITP”), and the HSI Special Agent Training (“HSISAT”) at the Federal Law

Enforcement Training Center in Glynco, Georgia. I have participated in the execution of previous search warrants, which involved child exploitation and/or child pornography offenses, and the search and seizure of computers, related peripherals, and computer media equipment. I am a member of the Seattle Internet Crimes Against Children Task Force ("ICAC"), and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

### **PURPOSE OF THE AFFIDAVIT**

3. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the following:

a. The property located at 2224 202<sup>nd</sup> St SW, Lynnwood, WA 98036 (hereinafter the SUBJECT PREMISES), more fully described in Attachment A, which is attached and incorporated herein by reference and the content of electronic storage devices located thereon, for the items more specifically described in Attachment B of this Affidavit.

b. The person of Christopher Robinson-Holm (SUBJECT PERSON), more fully described in Attachment A, which is attached and incorporated herein by reference;

c. A white Ford F-150 (WA License Plate 56677C) previously registered to the SUBJECT PERSON (SUBJECT VEHICLE), more fully described in Attachment A, which is attached and incorporated herein by reference.

4. As set forth below, there is probable cause to believe the SUBJECT PERSON at the SUBJECT PREMISES used a specific chat messaging platform to entice a minor and obtain visual depictions of minors engaged in sexually explicit conduct. There is, therefore, probable cause to believe that the SUBJECT PREMISES, VEHICLE and PERSON will contain evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography), 18 U.S.C. § 2422(b) (Enticement of a Minor), and 18 U.S.C. § 2252(a)(2), (b)(1) (Receipt/Distribution of Child Pornography), as well as attempt/conspiracy to commit such offenses, the

1 TARGET OFFENSES. I seek authorization to search and seize the items specified in  
2 Attachment B, which is incorporated herein by reference.

3 5. The facts set forth in this Affidavit are based on my own personal  
4 knowledge; knowledge obtained from other individuals during my participation in this  
5 investigation, including other law enforcement officers; review of documents and records  
6 related to this investigation; communications with others who have personal knowledge  
7 of the events and circumstances described herein; and information gained through my  
8 training and experience.

9 6. Because this affidavit is submitted for the limited purpose of establishing  
10 probable cause in support of the application for a search warrant, it does not set forth  
11 each and every fact that I or others have learned during the course of this investigation. I  
12 have set forth only the facts that I believe are relevant to the determination of probable  
13 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C.  
14 § 2251(a), (e) (Production of Child Pornography), 18 U.S.C. § 2422(b) (Enticement of a  
15 Minor), 18 U.S.C. § 1470 (Transfer of Obscene Material to Minors), and 18 U.S.C.  
16 § 2252(a)(2), (b)(1) (Receipt/Distribution of Child Pornography), will be found at the  
17 SUBJECT PREMISES or on the SUBJECT PERSON, or in the SUBJECT VEHICLES.

18 7. This Affidavit is being presented electronically pursuant to Local Criminal  
19 Rule CrR 41(d)(3).

## 20 **BACKGROUND ON DISCORD**

21 8. Discord is a voice, video, media and text (chat) communication  
22 service/platform in which users can communicate in private chats, ranging from 1–10  
23 users, or as part of a larger group/community called servers. Servers are also broken  
24 down into subcategories, or channels. Discord is headquartered in San Francisco,  
25 California.

## 26 **BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE**

27 9. In August 2022, Homeland Security Investigations (HSI) Tulsa received  
28 information from the Tulsa County District Attorney's Office regarding a possible victim

1 of exploitation via the Discord application. HSI Tulsa followed up with the reporting  
 2 party who stated that she had located chat conversations that were sexual in nature on  
 3 Discord between multiple users and the minor victim (MV). MV is under the age of  
 4 twelve years old. HSI Tulsa Special Agents (SAs) met with the mother of MV, who  
 5 allowed agents to take over MV's Discord account in furtherance of the investigation.

6 10. On or about August 17, 2022, MV's mother provided a statement to HSI  
 7 Special Agent (SA) Carder. MV's mother stated that earlier in 2022, MV was in the  
 8 bathroom for a long time and when she came out, the mother asked to see MV's phone.  
 9 MV's mother found that MV had been using the Discord app and had sent nude images  
 10 of herself with her face visible to an unidentified male. At that time, MV's parents wiped  
 11 MV's phone, removed all apps and restricted MV's access. MV's parents implemented  
 12 rules that MV was not allowed to have her phone in the bathroom with the door closed,  
 13 and MV cannot have her phone in her bedroom.

14 11. On or about August 9, 2022, MV's mother walked into MV's bedroom and  
 15 saw that MV was using her computer. MV told her mother that she was on the Discord  
 16 app, and MV's mother recognized MV's screen name as "pup." MV's mother saw there  
 17 were multiple conversations with multiple individuals that seemed to be sexual in nature.

18 12. On or about September 27, 2022, HSI Tulsa SAs obtained a search warrant  
 19 for MV's Discord account and located numerous targets who received images of MV's  
 20 vagina. One of the users was identified as "Bravo73#0073". The chat between MV and  
 21 "Bravo73#0073" appears to have taken place between approximately June 16, 2022, and  
 22 June 21, 2022. An excerpt of the transcript of the chat between MV and "Bravo73#0073"  
 23 from June 16, 2022, is as follows:

24 **Bravo73#0073:** ayo [Timestamp of message is 06/16/2022 08:20:44]

25 **Bravo73#0073:** What's your type

26 **Bravo73#0073:** I got hella hoes so I can give you gay panic

27 **MV:** Any

28 **MV:** Idc [I don't care]



1 **MV:** Well a good body

2 **Bravo73#0073:** Okay

3 **Bravo73#0073:** [Bravo73#0073 sends image of female kneeling on her hands and  
4 knees facing away from the camera with long black hair. The female is wearing a  
5 light blue lingerie romper with lace trim. The back of the romper shorts have been  
6 pulled up to expose the females buttocks.]

7 **Bravo73#0073:** My girl Madison

8 **Bravo73#0073:** She's a lot of fun

9 **MV:** MOMMY

10 **MV:** Mommy

11 **Bravo73#0073:** You wanna talk about gorilla grip

12 **MV:** ?

13 **Bravo73#0073:** I'm trying to say she really tight

14 **Bravo73#0073:** [Bravo73#0073 sends image of a female wearing a white tank top  
15 and dark colored thong and high heel shoes. The female is leaning forward against  
16 a wall, exposing her backside and looking back over her shoulder at the camera.]

17 **Bravo73#0073:** This is one of my actually close friends sky

18 **Bravo73#0073:** She's a lot of fun to fuck

19 **MV:** Mommy

20 **Bravo73#0073:** She loves butt stuff and having fun with other

21 **MV:** Fuck I'm horny nowww

22 **MV:** Ahhhhhh

23 **Bravo73#0073:** I have videos of me and others

24 **MV:** What!??

25 **Bravo73#0073:** Yeah

26 **Bravo73#0073:** Would that be something you'd wanna see?

27 **MV:** Wasssss

28 **MV:** Yessdd

1 **Bravo73#0073:** I have a nice one of a cute blonde choking on my cock

2 **Bravo73#0073:** Wanna see?

3 **MV:** Yessss

4 **Bravo73#0073:** [Bravo73#0073 sends a video depicting a blonde female  
5 performing oral sex on a male's erect penis. The video is approximately 10  
6 seconds long.]

7 **Bravo73#0073:** She dresses up for me so I get a personal slut in heels and a skirt

8 **Bravo73#0073:** She can barley take it

9 **MV:** Damn

10 **Bravo73#0073:** Whatcha think

11 **MV:** Ur big that's one thing

12 **Bravo73#0073:** Why thank you

13 **Bravo73#0073:** The first time her and I ever tried to fuck it wouldn't fit

14 **Bravo73#0073:** It really turns me on when someone talks about my size

15 **Bravo73#0073:** I have a video of her riding it as well

16 **Bravo73#0073:** I'm guessing you're having fun with all that

17 **MV:** Ur big that's one thing

18 **Bravo73#0073:** You said that lol

19 **MV:** Ur big

20 **Bravo73#0073:** Like it?

21 **MV:** Yea

22 **MV:** -

23 **Bravo73#0073:** When you turn 18 you should come out and have some fun with  
24 us

25 **MV:** Yea

26 **MV:** I should

27 **Bravo73#0073:** Don't worry we'll take care of you

28 **Bravo73#0073:** And are you mesmerized by the size

1 MV: Yea

2 MV: Could u tease me a lil pls

3 MV: Pls

4 MV: Plsss

5 **Bravo73#0073**: How so

6 MV: Just say things like faster and how much of a good girl I am

7 **Bravo73#0073**: Oh I want you to slow down

8 MV: Ok

9 **Bravo73#0073**: Slowly rub it.

10 **Bravo73#0073**: Now slowly speed up

11 **Bravo73#0073**: Faster and faster

12 **Bravo73#0073**: Good girl

13 **Bravo73#0073**: Faster

14 **Bravo73#0073**: Think about how it would feel

15 MV: Uhh fuck I wanna be ur good girl

16 **Bravo73#0073**: Just you wait. When the times right you'll be out here

17 MV: Yea

18 MV: And when u am I want U to make me a mess

19 **Bravo73#0073**: Oh you're guaranteed to be one

20 **Bravo73#0073**: You won't know how to walk

21 **Bravo73#0073**: Sky fell on my stairs because her legs were shaking to much

22 MV: Fuck I wanna be a good lil slut for u

23 **Bravo73#0073**: Your soul purpose would be to just take it

24 MV: Yes sir

25 **Bravo73#0073**: What's goin on with your snap?

26 MV: It wouldn't let me login

27 MV: Hold on

28 MV: Idk



1 **MV:** It's not working

2 **Bravo73#0073:** Do you have insta

3 **MV:** No

4 **MV:** I can give u pictures tho

5 **Bravo73#0073:** You sure?

6 **MV:** Yea

7 **Bravo73#0073:** Only send what you want

8 **MV:** [MV sends 4 images of a female that appears to resemble MV based on the  
9 victim identification conducted by HSI Tulsa.

10 **Image 1** depicts a female standing in a loose gray t-shirt with a pink or red logo on  
11 the upper left chest of the shirt, and navy sweatpants. The female is lifting the shirt  
12 to expose part of her abdomen. The female's face is not visible in the photo due to  
13 the camera angle. There is a gray patterned rug and blue and white nightstand seen  
14 in the background of the photo.

15 **Image 2** depicts a female with mid-length brown hair wearing a purple t-shirt with  
16 what appears to be an anime character printed on it. The female's face is visible in  
17 the image. The female appears to be between the ages of approximately 11-13  
18 years old due to the female's size and youthful facial features. The female in the  
19 photo has been determined to be MV based on the victim identification conducted  
20 by HSI Tulsa. The MV appears to be reclined on her back on a bed with a yellow  
21 and white patterned pillow and a lavender colored pillow behind her. The image  
22 appears to be using a digital filter such as the filters used in applications such as  
23 SnapChat. The filter casts white heart outlines and "Babe" over the female's face.

24 **Image 3** depicts MV with what appears to be another filter cast on her face with  
25 brown freckles and white outlines of the cartoon character "Hello Kitty". MV is  
26 wearing a gray shirt and is looking up to the left side.

27 **Image 4** depicts a female standing in a gray sports bra and navy sweatpants with a  
28 black long sleeve jacket left open to expose the female's abdomen. The angle of

1 the photo appears to be taken from above with the frame of the image from the  
2 female's chest to the ground, without the female's face visible. The same gray  
3 patterned rug and nightstand shown in the background of Image 1 is visible in the  
4 background.]

5 **MV:** There

6 **MV:** U can show the body ones to others but not the face pls

7 **Bravo73#0073:** And you're comfortable with all of this?

8 **MV:** Yea

9 **MV:** I'm horny ok

10 **Bravo73#0073:** I hope you know what ever you send me stays with me and only  
11 me

12 **MV:** Ok

13 **Bravo73#0073:** I don't share stuff unless it what we specifically talk about

14 **Bravo73#0073:** Those three I sent you all know and are okay with it

15 **MV:** Ok

16 **Bravo73#0073:** And you're 5'1?

17 **MV:** Yea

18 **MV:** Are the girls gay?

19 **MV:** Or sum

20 **Bravo73#0073:** They're all bi

21 **MV:** Thank god

22 **Bravo73#0073:** The one blowing me I've had a three way with

23 **MV:** Idk if I could do a good blow job with yours

24 **Bravo73#0073:** If it's that big in your mouth just wait til you try to take it

25 **MV:** I'll try

26 **Bravo73#0073:** I have lots of lube

27 **MV:** Do I have permission to cum

28 **Bravo73#0073:** Not yet

1 **Bravo73#0073:** Go much faster

2 **Bravo73#0073:** Faster

3 **Bravo73#0073:** Now cum

4 **MV:** I squirted

5 **Bravo73#0073:** Squirting is so hot

6 **MV:** Wanna see the mess I made

7 **Bravo73#0073:** Yes

8 **MV:** [MV sends an image depicting a female's vaginal area and pubic hair with  
9 the female's legs spread apart. The female appears to be on a bed with a pile of  
10 bedding at the top of the photo. The focal area of the image is the female's vaginal  
11 area and what appears to be female ejaculate on the bedding. The lighting of the  
12 image is red, making it difficult to determine a skin tone or color of the bedspread  
13 in the image.]

14 **Bravo73#0073:** Now that's a good girl

15 **MV:** Can I go again

16 **MV:** Pls

17 **MV:** I wanna go again

18 **Bravo73#0073:** Yes you can

19 **MV:** Thank u

20 **MV:** Thank you

21 **Bravo73#0073:** Do it how ever you want

22 **MV:** Ok

23 **Bravo73#0073:** Make yourself feel good

24 **Bravo73#0073:** What're you thinking about

25 **MV:** U railing the shit out of me

26 **Bravo73#0073:** Details

27 **MV:** And making me cum over and over

28 **MV:** While I'm screaming

1 MV: And going really fast and heard

2 MV: Can I cum

3 Bravo73#0073: Yes of course

4 Bravo73#0073: Also I'm into bdsm and bondage

5 MV: Do u wanna see the mess I made this time

6 Bravo73#0073: Of course

7 MV: [MV sends an image depicting a bed with a large, circular, dark stain and  
8 two pillows at the top of the photo. The lighting in the photo appears to be similar  
9 to the previous image sent by MV with red lighting, making it difficult to  
10 determine the color of the bedding in the photo.]

11 Bravo73#0073: Oh dear

12 MV: Yea

13 Bravo73#0073: That's a big mess

14 Bravo73#0073: Good

15 MV: Ik

16 Bravo73#0073: Just how I like it

17 Bravo73#0073: How're you feeling

18 MV: I feel like my stomach hurts and my legs r about to give out

19 MV: So really good

20 Bravo73#0073: Good girl that's exactly what I wanted to hear

21 Bravo73#0073: Was this how you were expecting our convos to go

22 MV: No not at all

23 MV: U?

24 Bravo73#0073: Not one bit this is my first time doing this

25 Bravo73#0073: With like underage

26 Bravo73#0073: So I'm a bit nervous tbh

27 MV: How was it

28 MV: Lmao

1 **MV:** No need

2 **Bravo73#0073:** It was fun I really enjoyed it

3 **MV:** Was I better then some of the girls u fuck

4 **Bravo73#0073:** Yes

5 **Bravo73#0073:** And just wait till I train you

6 **MV:** Im happy to hear that

7 **Bravo73#0073:** When you turn 18 you're coming out here

8 **MV:** Yes sir

9 **Bravo73#0073:** I'm very excited to destroy you

10 **MV:** I can't wait

11 **Bravo73#0073:** What're you most excited about

12 **MV:** To be a hot mess and being destroyed

13 **Bravo73#0073:** After I destroy you you'd have someone's face in there eating it  
14 all up

15 **MV:** I'd like that

16 **MV:** I feel like shit now

17 **MV:** Lmao [Time stamp on chat 06/16/2022 09:52:10]

18 [The chat continues for approximately one more hour until approximately  
19 06/16/2022 10:51:24 before resuming at approximately 06/16/2022 13:14:12 and  
20 continuing intermittently until approximately 06/21/2022 07:08:25.]

21 In another exchange of messages beginning around approximately 6/16/2022  
22 16:33:52, the following conversation occurs:

23 **MV:** ngl ima lil horny

24 **Bravo73#0073:** Oh really now

25 **MV:** Yea-

26 **MV:** ...

27 **Bravo73#0073:** Do you own any skirts or dresses

28 **MV:** Yea

1 **MV:** Skirt

2 **Bravo73#0073:** What kind babe

3 **MV:** This kind [MV sends an image of a female shown from the chest to the mid-  
4 thigh, wearing a mid-thigh length pleated dark colored, plaid patterned skirt and a  
5 black t-shirt that has two red and white colored mushrooms printed on it. The  
6 image appears to be taken as a selfie in the reflection of a bathroom mirror where  
7 the sink faucet is visible.]

8 **Bravo73#0073:** Oh perfect

9 **MV:** For?

10 **Bravo73#0073:** Wear that and nothing underneath and we could do it anywhere

11 **MV:** But what if it's windy

12 **Bravo73#0073:** That's okay

13 **Bravo73#0073:** Other people won't touch you just me

14 **MV:** Ok

15 **Bravo73#0073:** What about heels

16 **MV:** I can but I don't really like them

17 **Bravo73#0073:** Just show me them you don't gotta wear them

18 **MV:** I don't have any

19 **MV:** Lmao

20 **MV:** I tried them once and never fucking again

21 **Bravo73#0073:** Why

22 **MV:** I like to run and be able it fuck someone up at all times I can't do that

23 **MV:** With fucking heels:))

24 **Bravo73#0073:** What if you wore them just for our time together

25 **Bravo73#0073:** I'll always protect you

26 **MV:** I'd have to get some

27 **Bravo73#0073:** What style would you want?



1 **MV:** [MV sends four images that appear to be stock photos of high heel combat  
2 style boots and black lace-up heels.]

3 **MV:** Stuff like this

4 **MV:** But more boot like

5 **Bravo73#0073:** I'd love to have you in a skirt and a pair of heels

6 **MV:** Ok

7 **Bravo73#0073:** Your whole purpose wearing that would be to please me and take  
8 it like a good girl

9 **MV:** Yea sir

10 **MV:** Fuck I'm really horny now-

11 **MV:** What's ur vision of a fun night out

12 **Bravo73#0073:** We go to dinner and under the table I play with your clit and get  
13 you nice and wet

14 **Bravo73#0073:** Then after that we go see a movie and if no one's around then we  
15 have some more fun in there

16 **Bravo73#0073:** On the drive home you suck my cock while I drive

17 **Bravo73#0073:** And then when we get home it's a ball gag in the mouth and I'll  
18 tie you up.

19 **MV:** Mine is getting drunk and going out somewhere like a party or something  
20 and just being the bad fucking bitch ik how to be and maybe get in a fight or two

21 **Bravo73#0073:** I thought you meant sex wise

22 **MV:** Lmao

23 **MV:** Well in general

24 **MV:** That's mine 10000%

25 **Bravo73#0073:** Going out drinking is always fun

26 **Bravo73#0073:** Fuck now I'm horny to

27 **MV:** Yea

28 **MV:** Lmao

1 **MV:** Someone is horny

2 **Bravo73#0073:** So are you

3 **MV:** I mean yea

4 **MV:** Lmao

5 **MV:** But im almost always horny

6 **Bravo73#0073:** Same

7 **Bravo73#0073:** I'll bust a nut and be ready to go again in a couple minutes

8 **MV:** I just don't show it and that's where the bitchy person and the bad Fucking  
9 bitch comes in Lmaoo

10 **MV:** I just don't wanna stop

11 **MV:** Lmao

12 **MV:** Like I'll cum and wanna right after

13 **Bravo73#0073:** That's me as well

14 **Bravo73#0073:** Just wait till your tight pussy is stretched onto my cock

15 **MV:** Fuckkkkkj

16 **MV:** Ur making me horny

17 **Bravo73#0073:** Do you wanna see just it

18 **MV:** Yes pls

19 **MV:** If u don't mind ofc

20 **Bravo73#0073:** [Bravo73#0073 sends an image of an erect male penis.]

21 **MV:** Holy shit

22 **MV:** Fuckkk

23 **Bravo73#0073:** Whatcha think

24 **MV:** What do u think I think

25 **Bravo73#0073:** I want you to tell me

26 **MV:** I really really like it and I want it in me

27 **Bravo73#0073:** You'll barely be able to handle it

28 **MV:** Bitch wanna Fucking bet!

1 **Bravo73#0073:** Yes

2 **MV:** I mean you'll be my first time

3 **Bravo73#0073:** With you pinned down to the bed as I sliding it all in I'll be in  
4 your guts. You'll be moaning and squirming as you're brought nothing but  
5 pleasure and ecstasy

6 **MV:** I'm so wet

7 **MV:** Fuck

8 **Bravo73#0073:** How wet

9 **MV:** Like dripping

10 **Bravo73#0073:** I really wanna eat you out

11 **MV:** Can I play with myself

12 **MV:** Pls

13 **Bravo73#0073:** Are you comfortable showing me?

14 **MV:** Idk

15 **MV:** I haven't shaved

16 **Bravo73#0073:** Oh I don't care about hair

17 **MV:** I can't shave bc my parents took it away

18 **MV:** Bc I was cutting myself with it

19 **MV:** Like I could use a fucking knife [Time stamp on chat is 6/16/2022 17:02:55]

20 13. Based on how the initial chats on Discord began, it appears that  
21 "Bravo73#0073" already knew that MV was a minor when the Discord chat was initiated.  
22 Before any images of MV were sent, "Bravo73#0073" tells MV, "When you turn 18 you  
23 should come out and have some fun with us." The photos sent to "Bravo73#0073"  
24 showing MV's face appear to be a female between the ages of 11 to 13 due to MV's size  
25 and youthful facial features. In total, "Bravo73#0073" received approximately eight  
26 images of MV's exposed vagina and two images of MV masturbating.

27 14. On or about October 20, 2022, HSI Tulsa sent a summons to Discord  
28 requesting subscriber information for username "Bravo73#0073". On the same date,

Discord provided the following information regarding the account associated with username "Bravo73#0073".

User ID: 588866509527449621

Verified Email: 2018chris@gmail.com

Phone Number: +1 425-501-0654

IP Addresses: 107.77.205.31 and 50.35.100.70

The data provided showed that IP address 107.77.205.31 accessed Discord on October 18, 2022, at approximately 20:13:15 UTC. IP address 50.35.100.70 accessed Discord on October 17, 2022, at approximately 01:27:09 UTC.

Payment information provided by Discord for username "Bravo73#0073" showed the billing name on the payment card as Christopher ROBINSON-Holm (SUBJECT PERSON) with an address of 2224 202<sup>nd</sup> Street SW, Lynnwood, Washington 98036 (SUBJECT PREMISES).

15. On or about October 24, 2022, HSI Tulsa sent a summons to Google requesting subscriber information related to the email 2018chris@gmail.com. On the same date, Google's response included the following information.

Google Account ID: 1012803712595

Name: Chris Holm

Given Name: Chris

Family Name: Holm

Email: 2018chris@gmail.com

Created on: 2011-01-01 20:08:49 Z

Last Updated Date: 2022-10-24 16:46:33 Z

Last Logins: 2022-10-24 16:46:33 Z, 2022-10-24 15:23:44 Z, 2022-10-24 05:17:59 Z

Recovery Email: slrobinson1@gmail.com

1        Recovery SMS: +1 425-501-0654

2  
3 Google also provided billing information for the subscriber of 2018chris@gmail.com  
4 with the name of the SUBJECT PERSON.

5        16. On or about October 24, 2022, HSI Tulsa sent a summons to AT&T for  
6 subscriber information for phone number 425-501-0654. On the same date, AT&T  
7 responded with the following information.

8        Name: Christopher Robinson Holm

9        Credit Address: 3000 184<sup>th</sup> St SW, Lynnwood, WA 98037

10       Customer Since: 12/23/2011

11       Account Number: 298055209121

12       Account Status: Active

13       IMSI: 310410023055709

14       MSISDN Active: 12/23/2011 – Current

15       Service Start Date: 12/23/2011

16       Dealer Info: 77AM6

17       Payment Type: Prepaid

18       17. The IP address 107.77.205.31 is serviced by AT&T. On or about October  
19 24, 2022, a summons was sent to AT&T for subscriber information relating to the IP  
20 address 107.77.205.31. On or about October 25, 2022, AT&T responded stating, “After  
21 conducting a thorough search on all identifiers listed in the legal demand, AT&T was  
22 unable to identify any information responsive to the Legal Demand.”

23       18. The IP address 50.35.100.70 is controlled by Ziplly Fiber. On or about  
24 October 24, 2022, a summons was sent to Ziplly Fiber requesting subscriber information  
25 relating to the IP address 50.35.100.70. On or about October 27, 2022, Ziplly Fiber’s  
26 response included the following data.

27       Account Holder: Chris Holm

28       Service/Billing Address: 2224 202<sup>nd</sup> St Lynnwood, WA 98036

1 Email Address: 2018chris@gmail.com

2 Length of service: 12/18/2020 - Present

3 19. Database checks revealed that the SUBJECT PERSON's Washington  
4 driver's license also has the same address as the SUBJECT PREMISES.

5 20. Based on my investigation to date, other residents at the SUBJECT  
6 PREMISES may include Timothy Joseph Robinson-Holm (XX/XX/1994), Hanako Iris  
7 Jones (XX/XX/1997), and Sandra Lynn Robinson (XX/XX/1962).

8 21. On December 21, 2022, Lynnwood Police Department Detective Arnett  
9 confirmed that the SUBJECT PERSON is currently employed with the City of Lynnwood  
10 and the only address listed on file for the SUBJECT PERSON is the SUBJECT  
11 PREMISES.

12 22. On January 27, 2023, the SUBJECT VEHICLE was seen parked in the  
13 driveway of the SUBJECT PREMISES.

14 23. Based on the aforementioned information, I believe it is likely that the  
15 SUBJECT PERSON is the Discord user "Bravo73#0073" and is residing at the  
16 SUBJECT PREMISES.

17  
18 **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

19 23. I have had both training and experience in the investigation of computer-  
20 related crimes. Based on my training, experience, and knowledge, I know the following:  
21  
22  
23  
24  
25  
26  
27  
28



1           a.       Computers and digital technology are the primary way in which  
2 individuals interested in child pornography interact with each other. Computers basically  
3 serve four functions in connection with child pornography: production, communication,  
4 distribution, and storage.

5           b.       Digital cameras and smartphones with cameras save photographs or  
6 videos as a digital file that can be directly transferred to a computer by connecting the  
7 camera or smartphone to the computer, using a cable or via wireless connections such as  
8 “Wi-Fi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may  
9 be stored on a removable memory card in the camera or smartphone. These memory  
10 cards are often large enough to store thousands of high-resolution photographs or videos.  
11

12           c.       A device known as a modem allows any computer to connect to  
13 another computer through the use of telephone, cable, or wireless connection. Mobile  
14 devices such as smartphones and tablet computers may also connect to other computers  
15 via wireless connections. Electronic contact can be made to literally millions of  
16 computers around the world. Child pornography can therefore be easily, inexpensively  
17 and anonymously (through electronic communications) produced, distributed, and  
18 received by anyone with access to a computer or smartphone.  
19

20           d.       The computer’s ability to store images in digital form makes the  
21 computer itself an ideal repository for child pornography. Electronic storage media of  
22 various types - to include computer hard drives, external hard drives, CDs, DVDs, and  
23 “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a  
24 port on the computer - can store thousands of images or videos at very high resolution. It  
25 is extremely easy for an individual to take a photo or a video with a digital camera or  
26 camera-bearing smartphone, upload that photo or video to a computer, and then copy it  
27 (or any other files on the computer) to any one of those media storage devices. Some  
28

1 media storage devices can easily be concealed and carried on an individual's person.  
2 Smartphones and/or mobile phones are also often carried on an individual's person.

3  
4 e. The Internet affords individuals several different venues for  
5 obtaining, viewing, and trading child pornography in a relatively secure and anonymous  
6 fashion.

7  
8 f. Individuals also use online resources to retrieve and store child  
9 pornography. Some online services allow a user to set up an account with a remote  
10 computing service that may provide email services and/or electronic storage of computer  
11 files in any variety of formats. A user can set up an online storage account (sometimes  
12 referred to as "cloud" storage) from any computer or smartphone with access to the  
13 Internet. Even in cases where online storage is used, however, evidence of child  
14 pornography can be found on the user's computer, smartphone, or external media in most  
15 cases.

16  
17 g. A growing phenomenon related to smartphones and other mobile  
18 computing devices is the use of mobile applications, also referred to as "apps." Apps  
19 consist of software downloaded onto mobile devices that enable users to perform a  
20 variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or  
21 playing a game – on a mobile device. Individuals commonly use such apps to receive,  
22 store, distribute, and advertise child pornography, to interact directly with other like-  
23 minded offenders or with potential minor victims, and to access cloud-storage services  
24 where child pornography may be stored.

25  
26 h. As is the case with most digital technology, communications by way  
27 of computer can be saved or stored on the computer used for these purposes. Storing this  
28 information can be intentional (i.e., by saving an email as a file on the computer or saving  
the location of one's favorite websites in, for example, "bookmarked" files) or  
unintentional. Digital information, such as the traces of the path of an electronic

1 communication, may also be automatically stored in many places (e.g., temporary files or  
2 ISP client software, among others). In addition to electronic communications, a  
3 computer user's Internet activities generally leave traces or "footprints" in the web cache  
4 and history files of the browser used. Such information is often maintained indefinitely  
5 until overwritten by other data.

6  
7 24. Based upon my knowledge, experience, and training in child pornography  
8 investigations, and the training and experience of other law enforcement officers with  
9 whom I have had discussions, I know that there are certain characteristics common to  
10 individuals who have a sexualized interest in children and depictions of children:

11 a. They may receive sexual gratification, stimulation, and satisfaction  
12 from contact with children; or from fantasies they may have viewing children engaged in  
13 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other  
14 visual media; or from literature describing such activity.

15 b. They may collect sexually explicit or suggestive materials in a  
16 variety of media, including photographs, magazines, motion pictures, videotapes, books,  
17 slides, and/or drawings or other visual media. Such individuals often times use these  
18 materials for their own sexual arousal and gratification. Further, they may use these  
19 materials to lower the inhibitions of children they are attempting to seduce, to arouse the  
20 selected child partner, or to demonstrate the desired sexual acts. These individuals may  
21 keep records, to include names, contact information, and/or dates of these interactions, of  
22 the children they have attempted to seduce, arouse, or with whom they have engaged in  
23 the desired sexual acts.

24  
25 c. They often maintain any "hard copies" of child pornographic  
26 material that is, their pictures, films, video tapes, magazines, negatives, photographs,  
27 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of  
28

1 their home or some other secure location. These individuals typically retain these “hard  
2 copies” of child pornographic material for many years, as they are highly valued.

3  
4 d. Likewise, they often maintain their child pornography collections  
5 that are in a digital or electronic format in a safe, secure and private environment, such as  
6 a computer and surrounding area. These collections are often maintained for several  
7 years and are kept close by, often at the individual’s residence or some otherwise easily  
8 accessible location, to enable the owner to view the collection, which is valued highly.

9 e. They also may correspond with and/or meet others to share  
10 information and materials; rarely destroy correspondence from other child pornography  
11 distributors/collectors; conceal such correspondence as they do their sexually explicit  
12 material; and often maintain lists of names, addresses, and telephone numbers of  
13 individuals with whom they have been in contact and who share the same interests in  
14 child pornography.

15  
16 f. They generally prefer not to be without their child pornography for  
17 any prolonged time period. This behavior has been documented by law enforcement  
18 officers involved in the investigation of child pornography throughout the world.  
19 Importantly, e-mail and cloud storage can be a convenient means by which individuals  
20 can access a collection of child pornography from any computer, at any location with  
21 Internet access. Such individuals therefore do not need to physically carry their  
22 collections with them but rather can access them electronically. Furthermore, these  
23 collections can be stored on email “cloud” servers, which allow users to store a large  
24 amount of material at no cost, and possibly reducing the amount of any evidence of any  
25 of that material on the users’ computer(s).

26 25. Even if such individuals use a portable device (such as a mobile phone) to  
27 access the Internet and child pornography, it is more likely than not that evidence of this  
28 access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment

1 A, including on digital devices other than the portable device (for reasons including the  
2 frequency of “backing up” or “synching” mobile phones to computers or other digital  
3 devices).

4 26. In addition to offenders who collect and store child pornography, law  
5 enforcement has encountered offenders who obtain child pornography from the internet,  
6 view the contents, and subsequently delete the contraband, often after engaging in self-  
7 gratification. In light of technological advancements, increasing Internet speeds and  
8 worldwide availability of child sexual exploitative material, this phenomenon offers the  
9 offender a sense of decreasing risk of being identified and/or apprehended with quantities  
10 of contraband. This type of consumer is commonly referred to as a ‘seek and delete’  
11 offender, knowing that the same or different contraband satisfying their interests remain  
12 easily discoverable and accessible online for future viewing and self-gratification. I  
13 know that, regardless of whether a person discards or collects child pornography he/she  
14 accesses for purposes of viewing and sexual gratification, evidence of such activity is  
15 likely to be found on computers and related digital devices, including storage media, used  
16 by the person. This evidence may include the files themselves, logs of account access  
17 events, contact lists of others engaged in trafficking of child pornography, backup files,  
18 and other electronic artifacts that may be forensically recoverable.

19 27. Given the above-stated facts and based on my knowledge, training and  
20 experience, along with my discussions with other law enforcement officers who  
21 investigate child exploitation crimes, I believe that the SUBJECT PERSON likely has a  
22 sexualized interest in children and depictions of children, and that the SUBJECT  
23 PREMISES/PERSON/VEHICLE(s) are likely to contain evidence, fruits, and  
24 instrumentalities of the TARGET OFFENSES.

25 **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

26 28. As described above and in Attachment B, this application seeks permission  
27 to search for evidence, fruits and/or instrumentalities that might be found, in whatever  
28

1 form they are found. One form in which the evidence, fruits, and/or instrumentalities  
2 might be found is data stored on digital devices<sup>1</sup> such as computer hard drives or other  
3 electronic storage media.<sup>2</sup> Thus, the warrant applied for would authorize the seizure of  
4 digital devices or other electronic storage media or, potentially, the copying of  
5 electronically stored information from digital devices or other electronic storage media,  
6 all under Rule 41(e)(2)(B).  
7

8       29. *Probable cause.* Based upon my review of the evidence gathered in this  
9 investigation, my review of data and records, information received from other agents and  
10 computer forensics examiners, and my training and experience, I submit that if a digital  
11 device or other electronic storage media is found during the search of the SUBJECT  
12 PREMISES/PERSON/VEHICLE(S), there is probable cause to believe that evidence,  
13 fruits, and/or instrumentalities of the TARGET OFFENSES will be stored on those  
14 digital devices or other electronic storage media. As noted above, I believe the  
15 SUBJECT PERSON has been using digital devices or electronic storage media to entice a  
16 minor, transfer obscene material to a minor, and receive child pornography. There is,  
17 therefore, probable cause to believe that evidence, fruits and/or instrumentalities of the  
18 TARGET OFFENSES exists and will be found on digital devices or other electronic  
19 storage media found in a search of the SUBJECT PREMISES/PERSON/VEHICLE(S),  
20 for at least the following reasons:  
21

22  
23 <sup>1</sup> ["Digital device" includes any device capable of processing and/or storing data in electronic form, including, but  
24 not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral  
25 input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable  
26 media, related communications devices such as modems, routers and switches, and electronic/digital security  
devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices,  
personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global  
positioning satellite devices (GPS), or portable media players.

27 <sup>2</sup> Electronic Storage media is any physical object upon which electronically stored information can be recorded.  
28 Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.



- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the search of the SUBJECT PREMISES/PERSON/VEHICLE(S)

1 because:  
2

3 a. Stored data can provide evidence of a file that was once on the digital  
4 device or other electronic storage media but has since been deleted or edited, or  
5 of a deleted portion of a file (such as a paragraph that has been deleted from a  
6 word processing file). Virtual memory paging systems can leave traces of  
7 information on the digital device or other electronic storage media that show  
8 what tasks and processes were recently active. Web browsers, e-mail  
9 programs, and chat programs store configuration information that can reveal  
10 information such as online nicknames and passwords. Operating systems can  
11 record additional information, such as the history of connections to other  
12 computers, the attachment of peripherals, the attachment of USB flash storage  
13 devices or other external storage media, and the times the digital device or  
14 other electronic storage media was in use. Computer file systems can record  
15 information about the dates files were created and the sequence in which they  
16 were created.

17 b. As explained herein, information stored within a computer and other  
18 electronic storage media may provide crucial evidence of the “who, what, why,  
19 when, where, and how” of the criminal conduct under investigation, thus  
20 enabling the United States to establish and prove each element or alternatively,  
21 to exclude the innocent from further suspicion. In my training and experience,  
22 information stored within a computer or storage media (e.g., registry  
23 information, communications, images and movies, transactional information,  
24 records of session times and durations, internet history, and anti-virus,  
25 spyware, and malware detection programs) can indicate who has used or  
26 controlled the computer or storage media. This “user attribution” evidence is  
27 analogous to the search for “indicia of occupancy” while executing a search  
28 warrant at a residence. The existence or absence of anti-virus, spyware, and  
malware detection programs may indicate whether the computer was remotely  
accessed, thus inculcating or exculpating the computer owner and/or others  
with direct physical access to the computer. Further, computer and storage  
media activity can indicate how and when the computer or storage media was  
accessed or used. For example, as described herein, computers typically  
contain information that log: computer user account session times and  
durations, computer activity associated with user accounts, electronic storage  
media that connected with the computer, and the IP addresses through which  
the computer accessed networks and the internet. Such information allows  
investigators to understand the chronological context of computer or electronic  
storage media access, use, and events relating to the crime under

1 investigation.<sup>3</sup> Additionally, some information stored within a computer or  
2 electronic storage media may provide crucial evidence relating to the physical  
3 location of other evidence and the suspect. For example, images stored on a  
4 computer may both show a particular location and have geolocation  
5 information incorporated into its file data. Such file data typically also  
6 contains information indicating when the file or image was created. The  
7 existence of such image files, along with external device connection logs, may  
8 also indicate the presence of additional electronic storage media (e.g., a digital  
9 camera or cellular phone with an incorporated camera). The geographic and  
10 timeline information described herein may either inculcate or exculpate the  
11 computer user. Last, information stored within a computer may provide  
12 relevant insight into the computer user's state of mind as it relates to the  
13 offense under investigation. For example, information within the computer  
14 may indicate the owner's motive and intent to commit a crime (e.g., internet  
15 searches indicating criminal planning), or consciousness of guilt (e.g., running  
16 a "wiping" program to destroy evidence on the computer or password  
17 protecting/encrypting such evidence in an effort to conceal it from law  
18 enforcement).

19 c. A person with appropriate familiarity with how a digital device or other  
20 electronic storage media works can, after examining this forensic evidence in  
21 its proper context, draw conclusions about how the digital device or other  
22 electronic storage media were used, the purpose of their use, who used them,  
23 and when.

24 d. The process of identifying the exact files, blocks, registry entries, logs, or  
25 other forms of forensic evidence on a digital device or other electronic storage  
26 media that are necessary to draw an accurate conclusion is a dynamic process.  
27 While it is possible to specify in advance the records to be sought, digital  
28 evidence is not always data that can be merely reviewed by a review team and  
passed along to investigators. Whether data stored on a computer is evidence  
may depend on other information stored on the computer and the application of  
knowledge about how a computer behaves. Therefore, contextual information  
necessary to understand other evidence also falls within the scope of the  
warrant.

---

<sup>3</sup> For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

## **REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS**

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

### **SEARCH TECHNIQUES**

32. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

33. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

34. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that

1 reasonably appear capable of containing data or items that fall within the scope of  
2 Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or  
3 other electronic storage media and/or forensic images, using the following procedures:

4 **A. Processing the Search Sites and Securing the Data.**

5  
6 a. Upon securing the physical search site, the search team will conduct an  
7 initial review of any digital devices or other electronic storage media located at  
8 the subject premises described in Attachment A that are capable of containing  
9 data or items that fall within the scope of Attachment B to this Affidavit, to  
10 determine if it is possible to secure the data contained on these devices onsite  
in a reasonable amount of time and without jeopardizing the ability to  
accurately preserve the data.

11 b. In order to examine the electronically stored information (“ESI”) in a  
12 forensically sound manner, law enforcement personnel with appropriate  
13 expertise will attempt to produce a complete forensic image, if possible and  
14 appropriate, of any digital device or other electronic storage media that is  
capable of containing data or items that fall within the scope of Attachment B  
to this Affidavit.<sup>4</sup>

15  
16 c. A forensic image may be created of either a physical drive or a logical  
17 drive. A physical drive is the actual physical hard drive that may be found in a  
18 typical computer. When law enforcement creates a forensic image of a  
19 physical drive, the image will contain every bit and byte on the physical drive.  
20 A logical drive, also known as a partition, is a dedicated area on a physical  
21 drive that may have a drive letter assigned (for example the c: and d: drives on  
22 a computer that actually contains only one physical hard drive). Therefore,  
creating an image of a logical drive does not include every bit and byte on the  
physical drive. Law enforcement will only create an image of physical or  
logical drives physically present on or within the subject device. Creating an  
image of the devices located at the search locations described in Attachment A

---

24 <sup>4</sup> The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or  
25 other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound,  
26 scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always  
27 necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to  
28 assist investigators in their search for digital evidence. Computer forensic examiners are needed because they  
generally have technological expertise that investigative agents do not possess. Computer forensic examiners,  
however, often lack the factual and investigative expertise that an investigative agent may possess on any given  
case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely  
together.



will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachment A that have previously connected to devices at other locations may contain data from those other locations.

d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

**B. Searching the Forensic Images.**

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

b. These methodologies, techniques and protocols may include the use of a "hash value" library to exclude normal operating system files that do not need to be further searched. OR - Agents may utilize hash values to exclude certain known files, such as the operating system and other routine software, from the search results.

**BIOMETRIC UNLOCK**

35. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

1           a. I know from my training and experience, as well as from  
2 information found in publicly available materials published by device  
3 manufacturers, that many electronic devices, particularly newer mobile devices  
4 and laptops, offer their users the ability to unlock the device through biometric  
5 features in lieu of a numeric or alphanumeric passcode or password. These  
6 biometric features include fingerprint scanners and facial recognition features.  
7 Some devices offer a combination of these biometric features, and the user of such  
8 devices can select which features they would like to utilize.

9           b. If a device is equipped with a fingerprint scanner, a user may enable  
10 the ability to unlock the device through his or her fingerprints. For example, Apple  
11 offers a feature called “Touch ID,” which allows a user to register up to five  
12 fingerprints that can unlock a device. Once a fingerprint is registered, a user can  
13 unlock the device by pressing the relevant finger to the device’s Touch ID sensor,  
14 which is found in the round button (often referred to as the “home” button) located  
15 at the bottom center of the front of the device. The fingerprint sensors found on  
16 devices produced by other manufacturers have different names but operate  
17 similarly to Touch ID.

18           c. If a device is equipped with a facial recognition feature, a user may  
19 enable the ability to unlock the device through his or her face, iris, or retina. For  
20 example, Apple offers a facial recognition feature called “Face ID.” During the  
21 Face ID registration process, the user holds the device in front of his or her face.  
22 The device’s camera then analyzes and records data based on the user’s facial  
23 characteristics. The device can then be unlocked if the camera detects a face with  
24 characteristics that match those of the registered face. Facial recognition features  
25 found on devices produced by other manufacturers have different names but  
26 operate similarly to Face ID.

27           d. While not as prolific on digital devices as fingerprint and facial-  
28 recognition features, both iris and retina scanning features exist for securing  
devices/data. The human iris, like a fingerprint, contains complex patterns that are  
unique and stable. Iris recognition technology uses mathematical pattern-  
recognition techniques to map the iris using infrared light. Similarly, retina  
scanning casts infrared light into a person’s eye to map the unique variations of a  
person’s retinal blood vessels. A user can register one or both eyes to be used to  
unlock a device with these features. To activate the feature, the user holds the  
device in front of his or her face while the device directs an infrared light toward  
the user’s face and activates an infrared sensitive camera to record data from the  
person’s eyes. The device is then unlocked if the camera detects the registered eye.

1 e. In my training and experience, users of electronic devices often  
2 enable the aforementioned biometric features because they are considered to be a  
3 more convenient way to unlock a device than by entering a numeric or  
4 alphanumeric passcode or password. Moreover, in some instances, biometric  
5 features are considered to be a more secure way to protect a device's contents.  
6 This is particularly true when the users of a device are engaged in criminal  
7 activities and thus have a heightened concern about securing the contents of a  
8 device.

9 f. As discussed in this affidavit, based on my training and experience I  
10 believe that one or more digital devices will be found during the search. The  
11 passcode or password that would unlock the device(s) subject to search under this  
12 warrant is not known to law enforcement. Thus, law enforcement personnel may  
13 not otherwise be able to access the data contained within the device(s), making the  
14 use of biometric features necessary to the execution of the search authorized by  
15 this warrant.

16 g. I also know from my training and experience, as well as from  
17 information found in publicly available materials including those published by  
18 device manufacturers, that biometric features will not unlock a device in some  
19 circumstances even if such features are enabled. This can occur when a device has  
20 been restarted, inactive, or has not been unlocked for a certain period of time. For  
21 example, Apple devices cannot be unlocked using Touch ID when (1) more than  
22 48 hours has elapsed since the device was last unlocked or (2) when the device has  
23 not been unlocked using a fingerprint for 4 hours *and* the passcode or password  
24 has not been entered in the last 156 hours. Biometric features from other brands  
25 carry similar restrictions. Thus, in the event law enforcement personnel encounter  
26 a locked device equipped with biometric features, the opportunity to unlock the  
27 device through a biometric feature may exist for only a short time.

28 h. In my training and experience, the person who is in possession of a  
device or has the device among his or her belongings at the time the device is  
found is likely a user of the device. However, in my training and experience, that  
person may not be the only user of the device, and may not be the only individual  
whose physical characteristics are among those that will unlock the device via  
biometric features. Furthermore, while physical proximity is an important factor  
in determining who is the user of a device, it is only one among many other factors  
that may exist.

36. Due to the foregoing, I request that if law enforcement personnel encounter  
a device that is subject to search and seizure pursuant to this warrant and may be


1 unlocked using one of the aforementioned biometric features, and if law enforcement  
2 reasonably believes the SUBJECT PERSON is a user of the device, then – for the  
3 purpose of attempting to unlock the device in order to search the contents as authorized  
4 by this warrant – law enforcement personnel shall be authorized to: (1) press or swipe the  
5 fingers (including thumbs) of such person to the fingerprint scanner of the device; and/or  
6 (2) hold the device in front of the face and open eyes of such person and activate the  
7 facial, iris, or retina recognition feature.

8       37. In pressing or swiping an individual's thumb or finger onto a device and in  
9 holding a device in front of an individual's face and open eyes, law enforcement may not  
10 use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically,  
11 law enforcement may use no more than objectively reasonable force in light of the facts  
12 and circumstances confronting them.

**CONCLUSION**

38. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of the TARGET OFFENSES will be found during a search of the SUBJECT PREMISES/PERSON/VEHICLES, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices or other electronic storage media found. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES/PERSON/VEHICLE(S), as well as any digital devices and electronic storage media located therein, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

39. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

  
Alaina Dussler  
Special Agent

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit this 7th day of March, 2023.

  
S. KATE VAUGHAN  
United States Magistrate Judge

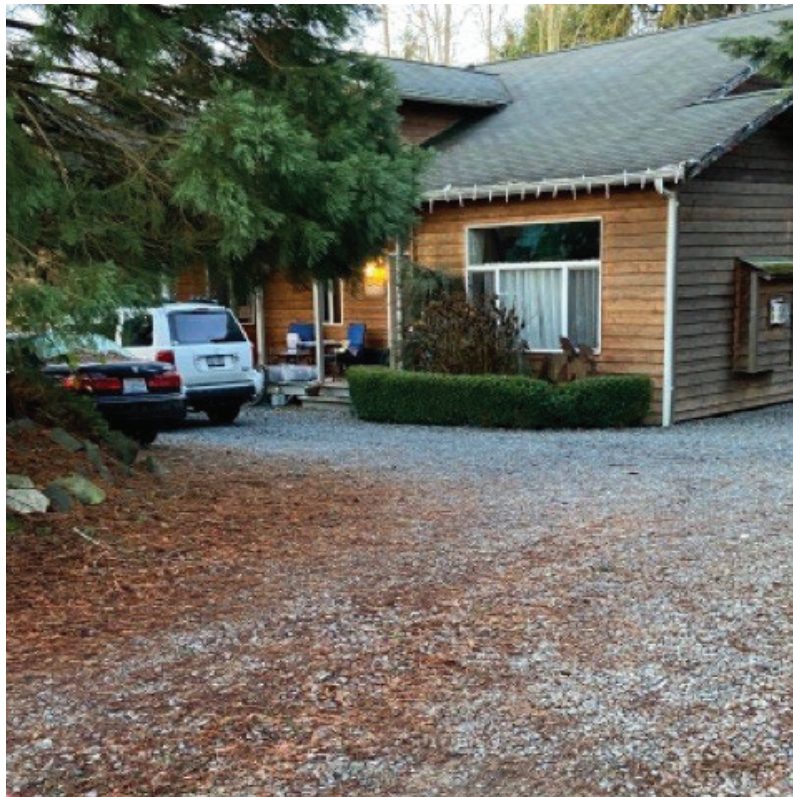


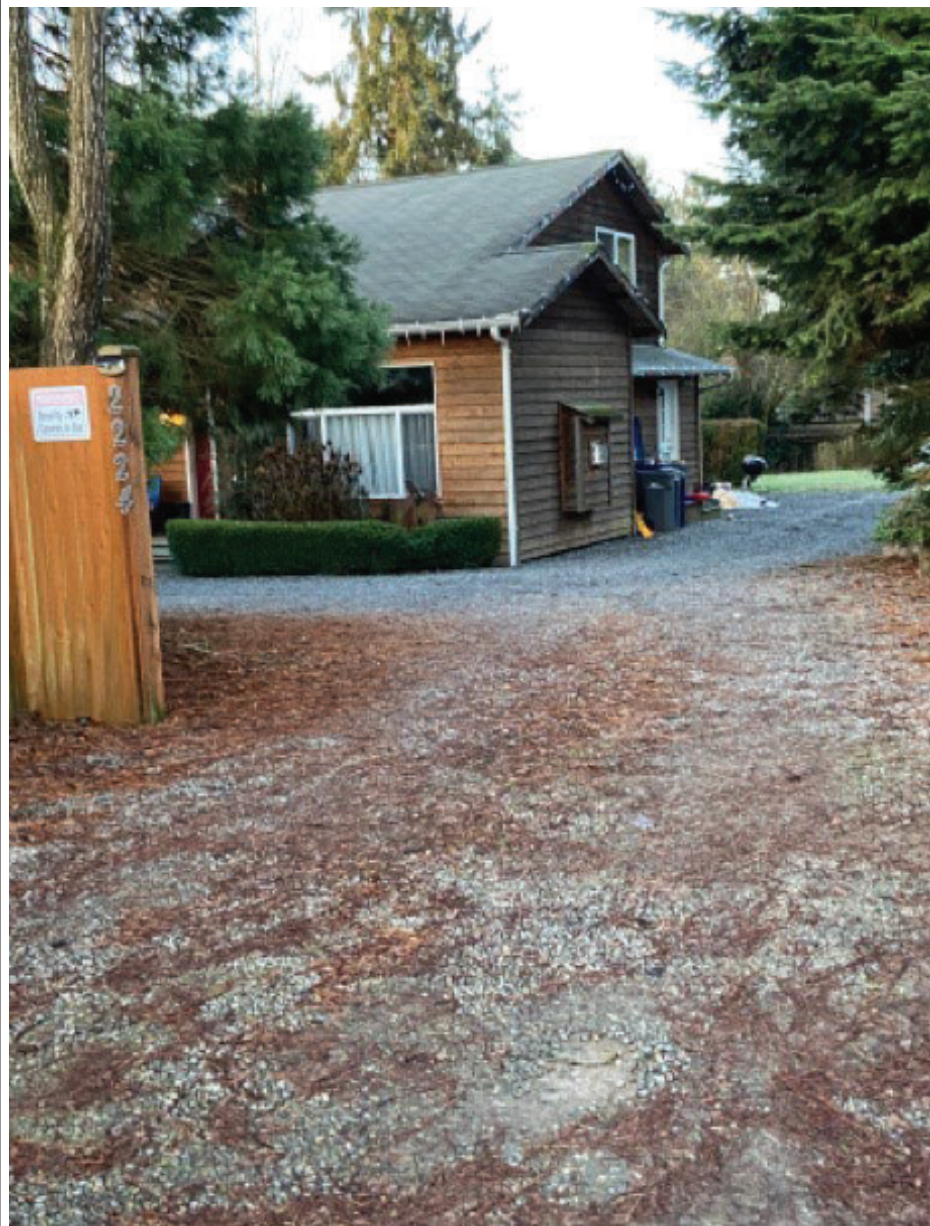
**ATTACHMENT A**

The SUBJECT PREMISES is the property located at 2242 202<sup>nd</sup> Street SW, Lynnwood, Washington, and contains is a two-story, single-family home. The building appears to be brown in color with stained wood siding and white trim. There is a covered front porch with white pillars and a red front door. A white side door to the SUBJECT PREMISES is also visible from the driveway on the right side of the house. The numbers “2224” are vertically affixed to the fence on the left side of the entrance of the driveway. The same numbers “2224” are affixed on a sign to the left of the red front door.

The search is to include the entirety of the residence, any garages or outbuildings located on the SUBJECT PREMISES, and any digital device(s) or other electronic storage media found.

However, if executing agents can reasonably determine onsite that a particular digital device or electronic storage medium is neither owned nor accessed by the SUBJECT PERSON, this warrant **DOES NOT** authorize its seizure or search.





ATTACHMENTS - 2  
USAO 2023R00040#

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE 5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970





ATTACHMENTS - 3  
USAO 2023R00040#

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE 5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970





1 The SUBJECT PERSON is CHRISTOPHER ROBINSON-HOLM, date of birth XX/XX/1998.



15  
16 The search is to include the SUBJECT PERSON and any backpacks, bags, or  
17 other containers that the SUBJECT PERSON may be capable of carrying, as well as any  
18 digital devices or electronic storage media found.

19  
20  
21  
22  
23  
24  
25  
26  
27  
28

SUBJECT VEHICLE 1

The SUBJECT VEHICLE is a 2001 white Ford F-150 pick-up truck bearing Washington license plate C43130R, Vehicle Identification Number 2FTZF17291CA02004.



The search is to include the entirety of the car and any closed containers, as well as any digital devices or electronic storage media found therein.

**ATTACHMENT B**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of violations 18 U.S.C. § 2251(a), (e) (Production of Child Pornography), 18 U.S.C. § 2422(b) (Enticement of a Minor), and 18 U.S.C. § 2252(a)(2), (b)(1) (Receipt/Distribution of Child Pornography), as well as attempt/conspiracy to commit those offenses (the TARGET OFFENSES):

1. Documents, records, and things that constitute evidence of who exercises dominion and control over the SUBJECT PREMISES or SUBJECT VEHICLE(S)..
2. All records relating to violations of the TARGET OFFENSES, including:
3.
  - a. visual depictions of minors engaged in sexually explicit conduct
  - b. identifying information for any individuals shown in such depictions or evidence that would otherwise assist in the identification of those depicted or those responsible for creating such visual depictions
  - c. information concerning the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct
  - d. information identifying the source of any visual depictions of minors engaged in sexually explicit conduct
  - e. evidence of communications related to the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct
  - f. evidence of contact with or communications about minors

1 g. evidence indicative of a sexualized interest in minors or depictions  
2 of minors

3 h. evidence of the use of Discord

4 4. Digital devices<sup>5</sup> or other electronic storage media<sup>6</sup> and/or their components,  
5 which include:

6 a. Any digital device or other electronic storage media capable of being  
7 used to commit, further, or store evidence of the offenses listed above;

8 b. Any digital devices or other electronic storage media used to  
9 facilitate the transmission, creation, display, encoding or storage of data, including word  
10 processing equipment, modems, docking stations, monitors, cameras, printers, plotters,  
11 encryption devices, and optical scanners;

12 c. Any magnetic, electronic or optical storage device capable of storing  
13 data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical  
14 disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic  
15 dialers, electronic notebooks, and personal digital assistants;

16 d. Any documentation, operating logs and reference manuals regarding  
17 the operation of the digital device or other electronic storage media or software;

18 e. Any applications, utility programs, compilers, interpreters, and other  
19 software used to facilitate direct or indirect communication with the computer hardware,  
20 storage devices, or data to be searched;

21 f. Any physical keys, encryption devices, dongles and similar physical  
22 items that are necessary to gain access to the computer equipment, storage devices or  
23 data; and

24 g. Any passwords, password files, test keys, encryption codes or other  
25 information necessary to access the computer equipment, storage devices or data.

26 <sup>5</sup> "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but  
27 not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral  
28 input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable  
media, related communications devices such as modems, routers and switches, and electronic/digital security  
devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices,  
personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global  
positioning satellite devices (GPS), or portable media players.

<sup>6</sup> Electronic Storage media is any physical object upon which electronically stored information can be recorded.

Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

1           5.     For any digital device or other electronic storage media upon which  
2 electronically stored information that is called for by this warrant may be contained, or  
3 that may contain things otherwise called for by this warrant:

4           a.     evidence of who used, owned, or controlled the digital device or  
5 other electronic storage media at the time the things described in this warrant were  
6 created, edited, or deleted, such as logs, registry entries, configuration files, saved  
7 usernames and passwords, documents, browsing history, user profiles, email, email  
8 contacts, "chat," instant messaging logs, photographs, and correspondence;

9           b.     evidence of software that would allow others to control the digital  
10 device or other electronic storage media, such as viruses, Trojan horses, and other forms  
11 of malicious software, as well as evidence of the presence or absence of security software  
12 designed to detect malicious software;

13           c.     evidence of the lack of such malicious software;

14           d.     evidence of the attachment to the digital device of other storage  
15 devices or similar containers for electronic evidence;

16           e.     evidence of counter-forensic programs (and associated data) that are  
17 designed to eliminate data from the digital device or other electronic storage media;

18           f.     evidence of the times the digital device or other electronic storage  
19 media was used;

20           g.     passwords, encryption keys, and other access devices that may be  
21 necessary to access the digital device or other electronic storage media;

22           h.     documentation and manuals that may be necessary to access the  
23 digital device or other electronic storage media or to conduct a forensic examination of  
24 the digital device or other electronic storage media;

25           i.     contextual information necessary to understand the evidence  
26 described in this attachment.

27           6.     Records and things evidencing the use of the internet, including:

28           a.     routers, modems, and network equipment used to connect computers  
to the Internet;

          b.     records of Internet Protocol addresses used;



1 c. records of Internet activity, including firewall logs, caches, browser  
2 history and cookies, “bookmarked” or “favorite” web pages, search terms that the user  
3 entered into any Internet search engine, and records of user-typed web addresses.  
4

5 7. During the execution of the search of the SUBJECT  
6 PREMISES/PERSON/VEHICLE(S) described in Attachment A, if law enforcement  
7 encounters a smartphone or other electronic device equipped with a biometric-unlock  
8 feature, and if law enforcement reasonably believes the SUBJECT PERSON is a user of  
9 the device, then – for the purpose of attempting to unlock the device in order to search the  
10 contents as authorized by this warrant – law enforcement personnel are authorized to: (1)  
11 press or swipe the fingers (including thumbs) of such person to the fingerprint scanner of  
12 the device; and/or (2) hold the device in front of the face and open eyes of such person  
13 and activate the facial, iris, or retina recognition feature.  
14

15 8. In pressing or swiping an individual’s thumb or finger onto a device and in  
16 holding a device in front of an individual’s face and open eyes, law enforcement may not  
17 use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically,  
18 law enforcement may use no more than objectively reasonable force in light of the facts  
19 and circumstances confronting them.  
20

21 THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE  
22 MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS  
23 SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO  
24 THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC  
25 STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL  
26 ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE  
27 CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR  
28 EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED  
CRIMES